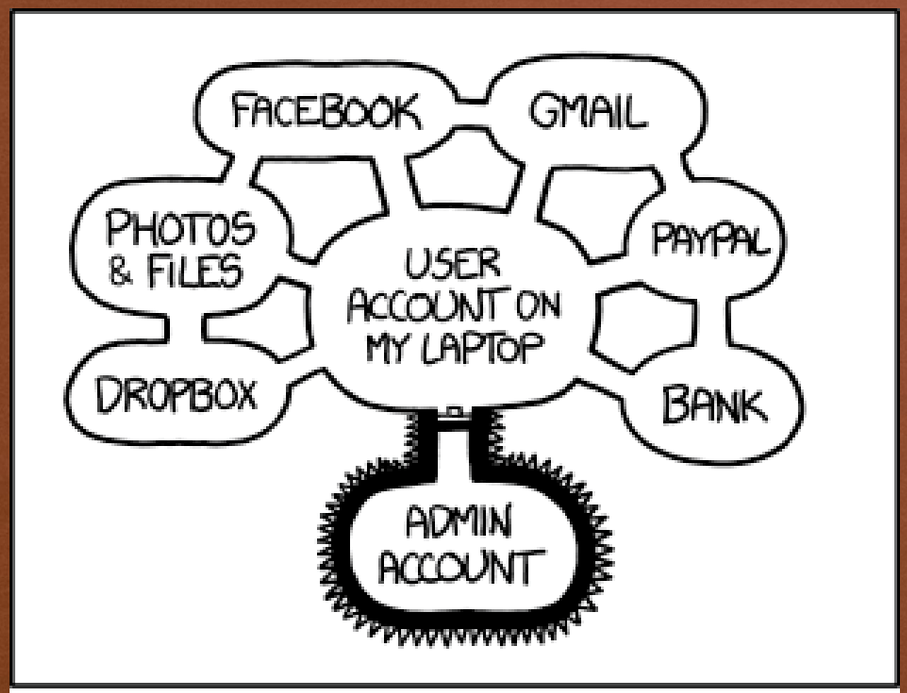
SECURITY

Chapter 8



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

https://xkcd.com/1200/

LEARNING OBJECTIVES

- Explain the difference between **authentication** and **authorization**
- Explain the use of a **hash function** to encrypt passwords on a computer system
- Describe **cyber-attacks** including viruses, worms, Trojan horses, DoS attacks, and phishing, and explain how they differ from each other

INTRODUCTION

- **Information security**
  - Keep information safe
  - Control access to authorized people only
- Physical security
  - lock doors
  - maintain control of devices
- Online security
  - Secure system programs
  - Secure operating system
  - Secure network

EXAMPLES OF SECURITY BREACHES

1. Someone hacked into a computer system that stored your **credit card details** and started buying stuff with your credit card number.

2. Someone managed to take over your computer and **lock you out**, asking for a **ransom payment** (or simply wiped your disk for fun).

3. Someone quietly used your computer to **send spam e-mails**, or they used it to attack other systems. Your IP address got blacklisted by a lot of ISPs.

4. Someone broke into your e-mail account and **sent a virus** to everyone in your address book.

EXAMPLES OF SECURITY BREACHES

Facebook–Cambridge Analytica data scandal, 2018

Cambridge Analytica, a data analysis firm that worked on President Trump's 2016 campaign, and its related company, Strategic Communications Laboratories (SCL), pilfered the data of 87 million Facebook users and secretly kept it.

The data had been provided by a third-party researcher Aleksandr Kogan of the company Global Science Research, a violation of Facebook's terms.

The “breach” freaked out thousands of people, and soon #deletefacebook was trending on Twitter.

EXAMPLES OF SECURITY BREACHES

WannaCry virus hits the NHS, 2017

Ransomware "WannaCry" was delivered via email attachment.

Clicking on the attachment made the virus spread through the computer locking up all the files and demanding payment in bitcoin before they could be accessed again.

More than 200,000 computers were infected with the virus across 150 countries.

A 22-year-old security researcher from Devon, Marcus Hutchins, managed to find the kill switch, after the NHS had been down for several days.

EXAMPLES OF SECURITY BREACHES

WannaCry virus hits the NHS, 2017

EXAMPLES OF SECURITY BREACHES

Hackers steal £650 million from global banks, 2015

For a period of two years, ending in early 2015, a group of hackers managed to gain access to secure information from more than 100 banking institutions around the world.

The cyber criminals used malware to infiltrate banks' computer systems and gather personal data.

They were then able to impersonate online bank staff to authorize fraudulent transfers, and even order ATM machines to dispense cash without a bank card.

It was estimated that around £650 million was stolen from the financial institutions in total.

THREATS AND DEFENSES

- Threats online are often more dangerous than threats to physical items
- Hackers prefer to attack easily accessible data

- Defenses : Multiple deterrents to attacks.
  - Authentication
    - process that establishes the user's identity to the satisfaction of the system.
  - Authorization
    - governs what an authenticated user is allowed to do.
  - Encryption
    - purpose is to make information meaningless even if someone does manage to steal it.

AUTHENTICATION

- **Authentication**: establishing identity
- Require usernames and passwords
- OS secures the password file with a **hash function**; one-way encryption

Example: password = badboy2

1. Replace letters by numbers: 2 1 4 2 15 25 2
2. Add digits: 2 + 1 + 4 + 2 + 15 + 25 + 2 = 51
3. Remainder of sum/7: 51 % 7 = 2 (modulo)
4. Add 1 and multiply by 9: (2 + 1) × 9 = 27
5. Reverse digits and convert to letters: 72 = gb

AUTHENTICATION

Given the hashed value of the password, can we get back the original string?

1. Reverse step 5. (Reverse digits and convert to letters)
   1. Convert letters to digits and reverse.
   2. g->7, b->2; reverse = 27.
2. Reverse step 4 (Add 1 and multiply by 9)
   1. Divide by 9 and subtract 1.
   2. 27/9 = 3 ; 3-1 = 2.
3. Reverse step 3 (Remainder of sum/7)
   1. Find sum such that sum%7 = 2
   2. Now we are stuck!!!

   This gives an infinite number of possibilities

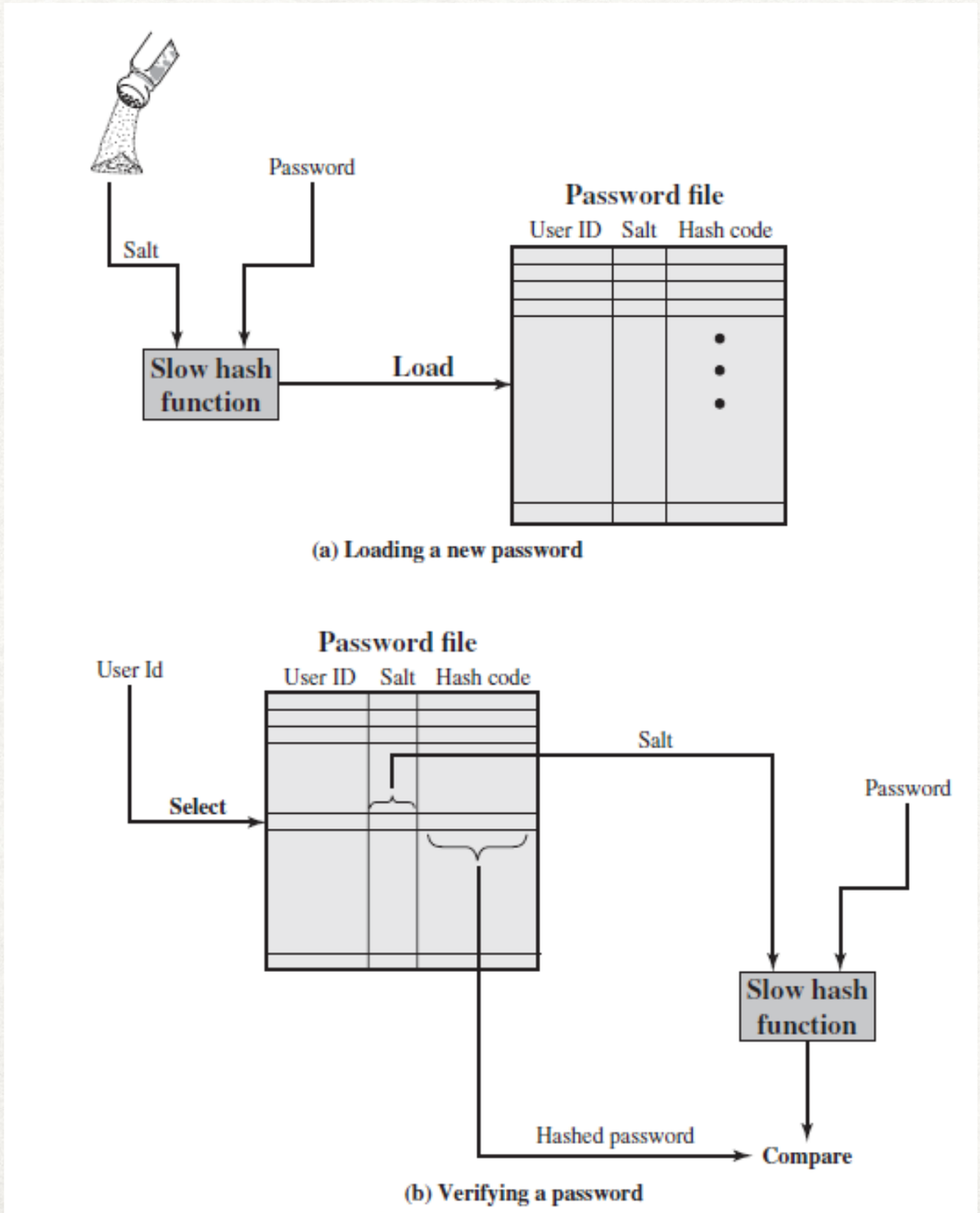
   9,16,30,37,44,51,58,65,72,79…….

In fact, there will be hundreds or thousands of strings that will all hash to “gb”

AUTHENTICATION

- Password file security: no plaintext password stored
- On login
  - Read username and password
  - Look up entry for username in a password file
  - Hash input password and compare
- What if two users end up choosing the same password?
  - Is this a problem?
- More secure method
  - Keep password creation time
  - Add creation time to password before hashing
  - Identical passwords won’t hash to identical values

AUTHENTICATION



THE USE OF HASHED PASSWORDS WITH SALT

The salt serves three purposes:

1. It prevents duplicate passwords from being visible in the password file.
2. It greatly increases the difficulty of offline dictionary attacks.
3. It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.

Figure Reference : *Computer Security Principles & Practice by Stallings & Brown*

AUTHENTICATION

- Password attacks
- Guess password, brute force or from knowledge
  - Try common passwords (e.g,123456)
  - Try personal references (e.g., pet name)
  - Try all possible passwords (computationally difficult)
- Steal password file and use **password-cracking software**
  - Tries words and word combinations, millions of password possibilities per second
- **Social engineering**: get a person to tell password

AUTHENTICATION

- Other authentication methods
- Answer personal information question
- Biometric information (fingerprint or retinal scans)
- One-time password scheme
  - User enters ID and a partial password
  - System or user device generates last half of the password
  - Last half of the password is good for only a few seconds
- **Dual authentication:** Temporary code or password is sent to a trusted device (e.g. two-factor token)

AUTHORIZATION

- **Authorization**: set of permitted actions for each authorized person

- Operating system maintains **access control lists**
  - Read access (read a file)
  - Write access (modify a file)
  - Execute access (run a program)
  - Delete access (remove a file)

- **System administrator** or **superuser** has universal access and sets up authorization

TYPES OF MALWARE

- **Malware**: malicious software arriving from the network
  - **Virus**: program embedded within another program or file, replicates itself and attacks other files (carried by infected host file)

  - **Worm**: program that can send copies of itself to other nodes on the network (self-replicating)

  - **Trojan horse**: program that seems beneficial but hides malicious code within it
    - ❑ **Keystroke logger**: records all keys typed
    - ❑ **Drive-by exploit/drive-by download**: Trojan horse downloaded by simply visiting an infected website

TYPES OF MALWARE

- **Denial-of-service (DoS) attack**: directs many computers try to access the same URL at the same time
  - Clogs the network, prevents legitimate access, and causes the server to crash
  - Distributed DoS uses thousands of computers
    - Uses a **zombie army** (**botnet**): many innocent computers infected with malware
- **Phishing**: obtain sensitive information by impersonating legitimate sources
  - Many emails; just a few “bites” are enough

TYPES OF HACKERS

White hats are security experts and those who work to help protect systems from attackers.
- Also called “ethical hackers”

Black hats are individuals or groups who work toward getting around security to steal information, get money, or do other nefarious, immoral, and illegal acts.

Grey hat hackers do not have malicious intentions. A Grey Hat will find vulnerabilities much like a White Hat but without permission to do so.

Past question on Malware

24. Which of the following statements are true about malware?

X. A virus is carried by an infected host file.
Y. The most common mechanism for spreading a virus is through email attachments.
Z. A worm is a self-replicating piece of software that does not need a host file to carry it.

A. X and Y only
B. X and Z only
C. Y and Z only
D. All of X, Y, and Z
E. None, or only one of X, Y, and Z

Past question on Malware

24. Which of the following statements are true about malware?

X. The most common mechanism for spreading a virus is through email attachments.
Y. Installing regular updates to an operating system is not good since it lowers the processor efficiency.
Z. A Trojan horse can hide a keystroke logger that captures user's passwords.

A. X only
B. Y only
C. Z only
D. None of X, Y, and Z
E. All, or two of X, Y, and Z